Network Management Card 3 (NMC 3) for Firmware v3.1.1.1 for Smart-UPS & v3.1.1.1 for 1-Phase Symmetra Release Notes

Table of Contents

The Smart-UPS application firmware v3.1.1.1/ 1-Phase Symmetra application firmware v3.1.1.1 release notes apply to the following NMC cards:

- AP9640 UPS Network Management Card 3
- AP9641 UPS Network Management Card 3
- AP9643 UPS Network Management Card 3

Affected Revision Levels

Top ↑

Component	File	Details
Smart-UPS Application	apc_hw21_su_ 3-1-1-1.nmc3	UPS Application for Smart-UPS, Smart-UPS RT, Smart-UPS VT, and MGE Galaxy 3500
Symmetra Application	apc_hw21_sy_ 3-1-1-1.nmc3	UPS Application for 1-Phase Symmetra and Symmetra LX

To upgrade to firmware version 3.0 or later, the only supported method is the Secure NMC System (SNS) Tool which can be downloaded from www.apc.com/secure-nmc or by searching for SFNMC3FMTSU and SFNMC3FMTSY. To access the firmware in the software, a valid Secure NMC subscription is required. For more information, see the SNS Tool User Guide.

NOTE: If you upgrade to firmware version 2.0 or later, you cannot downgrade to a firmware version lower than 2.0.

If you downgrade from firmware version 2.4+ to a firmware version lower than 2.4, this will cause the card to be formatted, erasing all security certificates, encryption keys, configuration settings, and the event and data logs.

Schneider Electric Device IP Configuration Wizard

The Device IP Configuration Wizard is a Windows application designed specifically to remotely configure the basic TCP/IP settings of Network Management Cards. The Wizard runs on Windows® Server 2012, Windows Server 2016, Windows Server 2019, Windows 8.1, and Windows 10. This utility is for IPv4 only.

NOTES:

- In firmware version v1.4.x and higher, it is not supported to assign IP addresses to Network Management Cards using the Wizard.
- You cannot search for assigned devices already on the network using an IP range unless you enable SNMPv1 and set the **Community Name** to “public”. For more information on SNMPv1, see the **User Guide**.
- When the NMC IP address settings are configured, to access the NMC Web UI in a browser, you must update the URL from http to http**s**.

The Wizard is available as a free download from the APC website at www.apc.com:

1. Go to https://www.apc.com/shop/us/en/tools/software-firmware and click **Show More** from the list of checkboxes in **Filter by > Software / Firmware**.
2. Select **Wizards and Configurators** to view the list of utilities available for download.
3. Click the Download button to download the **Device IP Configuration Wizard**.

New Features

Top ↑

New Feature	UPS Family	
	Smart-UPS	1-Phase Symmetra
Support added for user authentication via Lightweight Directory Access Protocol (LDAP).	♦	♦
Support added for baud rate 115,200 on the Console connection on Universal I/O port.	♦	♦
Support added for optional Spot Fluid Sensor (NBES0301).	♦	
Support added for configuring Universal I/O sensors via the `cfguio` command on the Command Line Interface (CLI).	♦	
Support added for remote authentication via the TACACS+ protocol. (Added for Smart-UPS application in v3.0).		♦
Security Update		
Support added for TLS 1.3.	♦	♦
Support added for SNMPv3 encryption via the SHA-256 and AES-256 protocols.	♦	♦
Password security has been updated to align with the requirements for IEC 62443-4-2. By default, passwords now need to be a minimum of 8 characters in length (strong password setting enabled). (Added for Smart-UPS application in v3.0)		♦

Fixed Issues

Top ↑

Fixed Issue	UPS Family	
	Smart-UPS	1-Phase Symmetra
Link-RX/TX LED is now working for all embedded NMC3s.	♦	
Dates in SNMP, such as upsAdvIdentDateOfManufacture, are now available in the correct format, mm/dd/yyyy.	♦	
The audit log of the Web UI is displayed in all supported languages.	♦	
The NMC3 Web UI now allows passwords with up to 64 characters, as expected. (Added for Smart-UPS application in v3.0)		♦

Fixed Issue	UPS Family	
	Smart-UPS	**1-Phase Symmetra**
For encrypted email settings, install CA certificate to the certificate store and set "Require CA Root Certificate" correctly. (Added for Smart-UPS application in v3.0)		♦
Improved TLS certificate for email. (Added for Smart-UPS application in v3.0)		♦
Security Update		
The following security vulnerability has been addressed in this release: CWE-327: Use of a Broken or Risky Cryptographic Algorithm. This software uses a broken or risky cryptographic algorithm or protocol. Removed support in SSH for diffie-hellman-group14-sha1.	♦	♦
The following third-party component has been updated to address cybersecurity vulnerabilities: • Wifi firmware: CVE-2020-24587 • Wifi firmware: CVE-2020-26146 Wi-Fi Device (AP9834) firmware v3.27.9 has been updated to correct this issue.	♦	♦
The following third-party component has been updated to address cybersecurity vulnerability: Treck stack: CVE-2020-10136	♦	♦
The following third-party component has been updated to address cybersecurity vulnerability: Treck HTTP Server: CVE-2020-25066	♦	♦
The following security vulnerability has been addressed in this release: CWE-598: Use of GET Request Method with Sensitive Query Strings. This software uses the HTTP GET method to process a request and includes sensitive information in the query string of that request. Configuration of HSTS is now independent from HTTP or HTTPS configuration. When HSTS is enabled, an STS header is added to all responses over HTTPS.	♦	♦
The following security vulnerability has been addressed in this release: CWE-307: Improper Restriction of Excessive Authentication Attempts. This software does not implement sufficient measures to prevent multiple failed authentication attempts within a short time frame, making it more susceptible to brute force attacks. The account now gets locked after bad login attempts.	♦	♦
The following security vulnerabilities have been addressed in this release: • CWE-523: Unprotected Transport of Credentials. Login pages do not use adequate measures to protect the user name and password while they are in transit from the client to the server. • CWE-319: Cleartext Transmission of Sensitive Information. The product transmits sensitive or security-critical data in cleartext in a communication channel that can be sniffed by unauthorized actors. **The user is now referred as an index rather than the user name NMC/KrtUvuh39YtQmHbyua297g/usercfg.htm?user=2.**	♦	♦

Fixed Issue	UPS Family	
	Smart-UPS	1-Phase Symmetra
The following security vulnerability has been addressed in this release: CWE-406: Insufficient Control of Network Message Volume (Network Amplification). The product does not sufficiently monitor or control transmitted network traffic volume, so that an actor can cause the product to transmit more traffic than should be allowed for that actor. SNMPv1/v2 is an insecure protocol and is disabled by default. SNMPv3 is available as an alternative. The NMC offers Access Control IP/DNS name configuration for SNMPv1/v2, as well as an internal configurable firewall to allow the user to further control network access.	♦	♦
The following security vulnerability has been addressed in this release: CWE-200: Exposure of Sensitive Information to An Unauthorized Actor SSH Cipher Block Chaining (CBC) cipher has been removed.	♦	♦
The following security vulnerabilities have been addressed in this release: • CWE-74: Improper neutralization of special elements in output used by a downstream component (Injection) • CWE-79: Improper neutralization of input during web page generation (Cross-site Scripting). (Added for Smart-UPS application in v3.0)		♦

Known Issues

Top ↑

Known Issue
There is no known issue in this release.

Miscellaneous

Top ↑

Recovering from a Lost Password

See the User Guide on the APC website for instructions on how to recover from a lost password.

Event Support List

To obtain the event names and event codes for all events supported by a currently connected APC device, first retrieve the config.ini file from the attached NMC. To use SCP to retrieve config.ini from a configured NMC:

1. Open a connection to the NMC, using its IP Address:
   scp <admin_username>@<ip_address>:config.ini <filename_to_be_stored>
2. Log on using the Administrator user name and password
3. Retrieve the config.ini file containing the settings of the NMC of the UPS:
   ftp > get config.ini

The file is written to the folder from which you launched SCP.

In the config.ini file, find the section heading [EventActionConfig]. In the list of events under that section heading, substitute 0x for the initial E in the code for any event to obtain the hexadecimal event code shown in the user interface and in the documentation. For example, the hexadecimal code for the code E0033 in the config.ini file (for the event "System: Configuration change") is 0x0033.

PowerNet MIB Reference Guide

NOTE: The MIB Reference Guide on the APC website explains the structure of the MIB, types of OIDs, and the procedure for defining SNMP trap receivers. For information on specific OIDs, use a MIB browser to view their definitions and available values directly from the MIB itself. You can view the definitions of traps at the end of the MIB itself (the file powernet441.mib on the APC website, www.apc.com).

Secure NMC System (SNS) Tool for Smart-UPS and 1-Phase Symmetra Hash Signatures

Signatures	**snst_nmc3_su_3-1-1-1.exe**	**snst_nmc3_sy_3-1-1-1.exe**
CRC32	B942777C	D27A0386
CRC64	31652D66CA563F60	59E741A408A55FDC
SHA-256	0591DC57366F71CBC93931C4B51F189F3FF88284825E2AC6A96DBD61150B64A6	37C88C579497B72891C6755498176BEA2EE26838E773D5D224679D5EE56641EA
SHA-1	7E558FCE90D056DB6A2D0F62F8F951B0FDE36035	7E5BB746D5968245D2B95924757F112B8A124776
BLAKE2sp	2B1EC5696500A7CE72718029A1FD58FACC568934D9BD560D51C39644D575C905	66A5E6825411DED6DFC40CCDC597B13EA6E38AEBD180B1029467476D625C9DEE

https://www.apc.com

990-6322Q-001

05-2024